

**WHAT IS CLAIMED IS:**

- 1           1.       A network device comprising:  
2           an access control list, wherein  
3                   said access control list comprises an access control list entry, and  
4                   said access control list entry comprises a user group field.
  
- 1           2.       The network device of claim 1, wherein  
2           said access control list comprises a plurality of access control list entries, and  
3           said access control list entries comprise said access control list entry.
  
- 1           3.       The network device of claim 2, wherein said access control list entry  
2 further comprises:  
3           a flow label field, wherein  
4                   said flow label field allows said access control list entry to be identified as  
5                   a role-based access control list (RBACL) entry.
  
- 1           4.       The network device of claim 2, wherein said access control list entry  
2 further comprises:  
3           a plurality of user group fields, wherein  
4                   said user group fields comprise said user group field.
  
- 1           5.       The network device of claim 4, wherein said user group fields further  
2 comprise:  
3           a source user group field; and  
4           a destination user group field.
  
- 1           6.       The network device of claim 5, wherein  
2           said source user group field stores a source user group identifier, and  
3           said source user group identifier identifies a user group of a source of a packet  
4                   processed using said access control list.

1           7.       The network device of claim 5, wherein  
2           said destination user group field stores a destination user group identifier, and  
3           said destination user group identifier identifies a user group of a destination of a  
4           packet processed using said access control list.

1           8.       A network device comprising:  
2           a forwarding table, wherein  
3                 said forwarding table comprises a plurality of forwarding table entries, and  
4                 at least one forwarding table entry of said forwarding table entries  
5                 comprises a user group field.

1           9.       The network device of claim 8, wherein said at least one forwarding table  
2   entry further comprises:  
3           a port identifier field, wherein  
4                 a port identifier stored in said port identifier field identifies a port.

1           10.      The network device of claim 9, wherein  
2           a user group, identified by a user group identifier stored in said user group field, is  
3           associated with said port.

1           11.      The network device of claim 10, wherein said at least one forwarding table  
2   entry further comprises:  
3           a media access control (MAC) address field configured to store a MAC address;  
4                 and  
5           a virtual local area network (VLAN) identifier field, wherein  
6                 a VLAN identifier stored in said VLAN identifier field identifies a VLAN,  
7                 and  
8                 a combination of said MAC address and said VLAN identifier identify said  
9                 port and a user group identified by a user group identifier stored in  
10                 said user group field.

1           12.    The network device of claim 10, wherein said at least one forwarding table  
2 entry further comprises:  
3           a media access control (MAC) address field configured to store a MAC address,  
4           wherein  
5           said MAC address is associated with a user group identified by a user  
6           group identifier stored in said user group field.

1           13.    The network device of claim 8, wherein said at least one forwarding table  
2 entry further comprises:  
3           a virtual local area network (VLAN) identifier field, wherein  
4           a VLAN identifier stored in said VLAN identifier field identifies a VLAN,  
5           and  
6           said VLAN is associated with a user group identified by a user group  
7           identifier stored in said user group field.

1           14.    A method comprising:  
2           comparing a user group of a packet with a user group of a destination of said  
3           packet.

1           15.    The method of claim 14, wherein  
2           said user group of said destination of said packet is identified by a user group  
3           identifier, and  
4           said user group identifier is stored in a role-based access control list entry of an  
5           access control list.

1           16.    The method of claim 14, wherein  
2           said user group of said packet is a source user group, and  
3           said user group of said destination of said packet is a destination user group.

1        17.    The method of claim 16, wherein  
 2        said source user group is assigned to a source of said packet based on a role of said  
 3        source, and  
 4        said destination user group is assigned to said destination based on a role of said  
 5        destination.

1        18.    The method of claim 16, further comprising:  
 2        retrieving said destination user group from a forwarding information base.

1        19.    The method of claim 18, further comprising:  
 2        storing said destination user group in an access control list.

1        20.    The method of claim 16, wherein  
 2        said source user group is indicated by a source user group identifier stored in said  
 3        packet, and  
 4        said destination user group is indicated by a destination user group stored in a  
 5        network device receiving said packet.

1        21.    The method of claim 16, further comprising:  
 2        determining said source user group; and  
 3        determining said destination user group by looking up said destination user group  
 4        in an access control list.

1        22.    The method of claim 21, wherein  
 2        said destination user group is identified by a destination user group identifier, and  
 3        said destination user group identifier is stored in a role-based access control list  
 4        entry of said access control list.

1        23.    The method of claim 21, wherein  
 2        said access control list is a role-based access control list.

1           24.    The method of claim 21, wherein said determining said source user group  
2 comprises:

3           extracting a source user group identifier from said packet, wherein  
4           said source user group identifier identifies said source user group.

1           25.    The method of claim 24, further comprising:  
2 populating said access control list with a destination user group identifier, wherein  
3           said destination user group identifier identifies said destination user group.

1           26.    The method of claim 25, wherein  
2 said destination user group is assigned to said destination based on a role of said  
3           destination.

1           27.    The method of claim 25, wherein  
2 said comparing and said populating are performed by a network device, and  
3 said populating comprises  
4           sending a request to another network device, and  
5           receiving a response from said another network device, wherein  
6           said response includes a destination user group identifier, and  
7           said destination user group identifier identifies said destination user  
8           group.

1           28.    The method of claim 14, further comprising:  
2 populating a forwarding table with a user group identifier, wherein  
3           said user group identifier identifies said user group of said packet, and  
4           said user group of said packet indicates a user group of a source of said  
5           packet.

1           29.    The method of claim 28, wherein  
2 said source user group is assigned to said source based on a role of said source.

1        30.     The method of claim 28, wherein  
 2        said user group is a source user group, and  
 3        said user group identifier is a source user group identifier.

1        31.     The method of claim 30, wherein  
 2        said comparing and said populating are performed by a network device, and  
 3        said populating comprises  
 4                determining said source user group.

1        32.     The method of claim 31, wherein said populating further comprises:  
 2        receiving an authentication message from another network device, wherein  
 3                said response includes said source user group identifier.

1        33.     A computer program product comprising:  
 2        a first set of instructions, executable on a computer system, configured to compare  
 3                a user group of a packet with a user group of a destination of said packet;  
 4                and  
 5        computer readable media, wherein said computer program product is encoded in  
 6                said computer readable media.

1        34.     The computer program product of claim 33, wherein  
 2        said user group of said packet is a source user group, and  
 3        said user group of said destination of said packet is a destination user group.

1        35.     The computer program product of claim 34, further comprising:  
 2        a second set of instructions, executable on said computer system, configured to  
 3                retrieve said destination user group from a forwarding information base.

1        36.     The computer program product of claim 35, further comprising:  
 2        a third set of instructions, executable on said computer system, configured to  
 3                storing said destination user group in an access control list.

1           37.     The computer program product of claim 33, wherein  
2           said source user group is indicated by a source user group identifier stored in said  
3           packet, and  
4           said destination user group is indicated by a destination user group stored in a  
5           network device receiving said packet.

1           38.     The computer program product of claim 34, further comprising:  
2           a second set of instructions, executable on said computer system, configured to  
3           determine said source user group; and  
4           a third set of instructions, executable on said computer system, configured to  
5           determine said destination user group by looking up said destination user  
6           group in an access control list.

1           39.     The computer program product of claim 38, wherein said second set of  
2           instructions comprises:  
3           a first subset of instructions, executable on said computer system, configured to  
4           extract a source user group identifier from said packet, wherein  
5           said source user group identifier identifies said source user group.

1           40.     The computer program product of claim 39, further comprising:  
2           a fourth set of instructions, executable on said computer system, configured to  
3           populate said access control list with a destination user group identifier,  
4           wherein  
5           said destination user group identifier identifies said destination user group.

1           41.     The computer program product of claim 33, further comprising:  
2           a second set of instructions, executable on said computer system, configured to  
3           populate a forwarding table with a user group identifier, wherein  
4           said user group identifier identifies said user group of said packet, and  
5           said user group of said packet indicates a user group of a source of said  
6           packet.

1           42.     The computer program product of claim 41, wherein said second set of  
2 instructions comprises:  
3           a first subset of instructions, executable on said computer system, configured to  
4           determine said source user group.

1           43.     The computer program product of claim 42, wherein said second set of  
2 instructions comprises:  
3           a second subset of instructions, executable on said computer system, configured to  
4           receive an authentication message from another network device, wherein  
5           said response includes said source user group identifier.

1           44.     An apparatus comprising:  
2 means for comparing a user group of a packet with a user group of a destination of  
3           said packet.

1           45.     The apparatus of claim 44, wherein  
2 said user group of said packet is a source user group, and  
3 said user group of said destination of said packet is a destination user group.

1           46.     The apparatus of claim 45, further comprising:  
2 means for retrieving said destination user group from a forwarding information  
3           base.

1           47.     The apparatus of claim 46, further comprising:  
2 means for storing said destination user group in an access control list.

1           48.     The apparatus of claim 45, wherein  
2 said source user group is indicated by a source user group identifier stored in said  
3           packet, and  
4 said destination user group is indicated by a destination user group stored in a  
5           network device receiving said packet.



1        49.     The apparatus of claim 45, further comprising:  
 2        means for determining said source user group; and  
 3        means for determining said destination user group by looking up said destination  
 4        user group in an access control list.

1        50.     The apparatus of claim 49, wherein said means for determining said source  
 2        user group comprises:  
 3        means for extracting a source user group identifier from said packet, wherein  
 4        said source user group identifier identifies said source user group.

1        51.     The apparatus of claim 50, further comprising:  
 2        means for populating said access control list with a destination user group  
 3        identifier, wherein  
 4        said destination user group identifier identifies said destination user group.

1        52.     The apparatus of claim 44, further comprising:  
 2        means for populating a forwarding table with a user group identifier, wherein  
 3        said user group identifier identifies said user group of said packet, and  
 4        said user group of said packet indicates a user group of a source of said  
 5        packet.

1        53.     The apparatus of claim 52, wherein  
 2        said means for comparing and said means for populating are included in a network  
 3        device, and  
 4        said means for populating comprises  
 5        determining said source user group.

1        54.     The apparatus of claim 53, wherein said means for populating further  
 2        comprises:  
 3        means for receiving an authentication message from another network device,  
 4        wherein  
 5        said response includes said source user group identifier.

1        55.    A method comprising:  
 2        populating an access control list with a destination user group identifier, wherein  
 3                said destination user group identifier identifies a destination user group of  
 4                a destination.

1        56.    The method of claim 55, wherein  
 2        said destination user group is assigned to said destination based on a role of said  
 3        destination.

1        57.    The method of claim 55, wherein  
 2        said populating is performed by a network device and comprises  
 3                sending a request to another network device, and  
 4                receiving a response from said another network device, wherein  
 5                        said response includes said destination user group identifier, and  
 6                        said destination user group identifier identifies said destination user  
 7                        group.

1        58.    The method of claim 55, further comprising:  
 2        comparing a user group of a packet with said destination user group.

1        59.    The method of claim 58, wherein  
 2        said user group of said packet is a source user group,  
 3        said destination user group is a user group of a destination of said packet, and  
 4        said destination is said destination of said packet.

1        60.    The method of claim 59, wherein  
 2        said source user group is assigned to a source of said packet based on a role of said  
 3                source, and  
 4        said destination user group is assigned to said destination based on a role of said  
 5        destination.

1        61.     The method of claim 59, wherein  
 2        said source user group is indicated by a source user group identifier stored in said  
 3        packet, and  
 4        said destination user group is indicated by a destination user group stored in a  
 5        network device receiving said packet.

1        62.     The method of claim 59, further comprising:  
 2        determining said source user group; and  
 3        determining said destination user group by looking up said destination user group  
 4        in an access control list.

1        63.     The method of claim 62, wherein  
 2        said access control list is a role-based access control list.

1        64.     The method of claim 62, wherein said determining said source user group  
 2 comprises:  
 3        extracting a source user group identifier from said packet, wherein  
 4        said source user group identifier identifies said source user group.

1        65.     A computer program product comprising:  
 2        a first set of instructions, executable on a computer system, configured to populate  
 3        an access control list with a destination user group identifier, wherein  
 4        said destination user group identifier identifies a destination user group of  
 5        a destination; and  
 6        computer readable media, wherein said computer program product is encoded in  
 7        said computer readable media.

1        66.     The computer program product of claim 65, further comprising:  
 2        a second set of instructions, executable on said computer system, configured to  
 3        compare a user group of a packet with said destination user group.

1        67.     The computer program product of claim 66, wherein  
 2        said user group of said packet is a source user group,  
 3        said destination user group is a user group of a destination of said packet, and  
 4        said destination is said destination of said packet.

1        68.     The computer program product of claim 67, further comprising:  
 2        a third set of instructions, executable on said computer system, configured to  
 3                determine said source user group; and  
 4        a fourth set of instructions, executable on said computer system, configured to  
 5                determine said destination user group by looking up said destination user  
 6                group in an access control list.

1        69.     The computer program product of claim 68, wherein said third set of  
 2        instructions comprises:  
 3                a first subset of instructions, executable on said computer system, configured to  
 4                extracting a source user group identifier from said packet, wherein  
 5                said source user group identifier identifies said source user group.

1        70.     An apparatus comprising:  
 2        means for populating an access control list with a destination user group identifier,  
 3                wherein  
 4                said destination user group identifier identifies a destination user group of  
 5                a destination.

1        71.     The apparatus of claim 70, further comprising:  
 2        means for comparing a user group of a packet with said destination user group.

1        72.     The apparatus of claim 71, wherein  
 2        said user group of said packet is a source user group,  
 3        said destination user group is a user group of a destination of said packet, and  
 4        said destination is said destination of said packet.

1        73.    The apparatus of claim 72, further comprising:  
 2        means for determining said source user group; and  
 3        means for determining said destination user group by looking up said destination  
 4        user group in an access control list.

1        74.    The apparatus of claim 73, wherein said means for determining said source  
 2        user group comprises:  
 3        means for extracting a source user group identifier from said packet, wherein  
 4        said source user group identifier identifies said source user group.

1        75.    A method comprising:  
 2        populating a forwarding table with a user group identifier.

1        76.    The method of claim 75, wherein  
 2        said user group identifier is a source user group identifier, and so identifies a  
 3        source user group.

1        77.    The method of claim 76, wherein  
 2        a source of a packet is in said source user group.

1        78.    The method of claim 77, wherein  
 2        said source user group is assigned to said source based on a role of said source.

1        79.    The method of claim 77, wherein said populating comprises  
 2        determining said source user group.

1        80.    The method of claim 79, wherein said populating is performed by a  
 2        network device and further comprises:  
 3        receiving an authentication message from another network device, wherein  
 4        said response includes said source user group identifier.

1        81.    The method of claim 77, wherein  
 2        a destination of said packet is in a destination user group.

1        82.    The method of claim 81, wherein  
2        said destination user group is assigned to said destination based on a role of said  
3        destination.

1        83.    The method of claim 81, further comprising:  
2        comparing a source user group of said packet with said destination user group.

1        84.    The method of claim 83, wherein  
2        said source user group of said packet is indicated by a source user group identifier  
3        stored in said packet, and  
4        said destination user group is indicated by a destination user group stored in a  
5        network device performing said comparison.

1        85.    The method of claim 81, further comprising:  
2        determining said source user group; and  
3        determining said destination user group by looking up said destination user group  
4        in an access control list stored at said network device performing said  
5        comparison.

1        86.    The method of claim 85, wherein said determining said source user group  
2        comprises:  
3        extracting said source user group identifier stored in said packet from said packet,  
4        wherein  
5        said source user group identifier stored in said packet identifies said source  
6        user group of said source of said packet.

1        87.     A computer program product comprising:  
 2        a first set of instructions, executable on a computer system, configured to populate  
 3        a forwarding table with a user group identifier, wherein  
 4        said user group identifier is a source user group identifier, and so identifies  
 5        a source user group; and  
 6        computer readable media, wherein said computer program product is encoded in  
 7        said computer readable media.

1        88.     The computer program product of claim 87, wherein said first set of  
 2        instructions comprises:  
 3        a first subset of instructions, executable on said computer system, configured to  
 4        determine said source user group.

1        89.     The computer program product of claim 88, wherein said first set of  
 2        instructions comprises:  
 3        a second subset of instructions, executable on said computer system, configured to  
 4        receive an authentication message from another network device, wherein  
 5        said response includes said source user group identifier.

1        90.     The computer program product of claim 87, wherein  
 2        a destination of said packet is in a destination user group.

1        91.     The computer program product of claim 90, further comprising:  
 2        a second set of instructions, executable on said computer system, configured to  
 3        determine said source user group; and  
 4        a third set of instructions, executable on said computer system, configured to  
 5        determine said destination user group by looking up said destination user  
 6        group in an access control list stored at said network device performing  
 7        said comparison.

1           92.    The computer program product of claim 91, wherein said second set of  
2 instructions comprises:  
3           a first subset of instructions, executable on said computer system, configured to  
4           extracting said source user group identifier stored in said packet from said  
5           packet, wherein  
6           said source user group identifier stored in said packet identifies said source  
7           user group of said source of said packet.

1           93.    An apparatus comprising:  
2 means for populating a forwarding table with a user group identifier, wherein  
3           said user group identifier is a source user group identifier, and so identifies  
4           a source user group.

1           94.    The apparatus of claim 93, wherein said means for populating comprises  
2 means for determining said source user group.

1           95.    The apparatus of claim 94, wherein said means for populating is performed  
2 by a network device and further comprises:  
3           means for receiving an authentication message from another network device,  
4           wherein  
5           said response includes said source user group identifier.

1           96.    The apparatus of claim 93, wherein  
2 a destination of said packet is in a destination user group.

1           97.    The apparatus of claim 94, further comprising:  
2 means for determining said source user group; and  
3 means for determining said destination user group by looking up said destination  
4           user group in an access control list stored at said network device  
5           performing said comparison.



1           98.     The apparatus of claim 97, wherein said means for determining said source  
2 user group comprises:  
3           means for extracting said source user group identifier stored in said packet from  
4           said packet, wherein  
5           said source user group identifier stored in said packet identifies said source  
6           user group of said source of said packet.

1           99.     A method comprising:  
2           indexing a row of a permissions matrix with a first user group; and  
3           indexing a column of said permissions matrix with a second user group.

1           100.    The method of claim 99, wherein  
2           said first user group is a source user group, and  
3           said second user group is a destination user group.

1           101.    The method of claim 100, wherein said permissions matrix comprises:  
2           a plurality of permissions matrix entries.

1           102.    The method of claim 101, wherein  
2           each of said permissions matrix entries is a pointer to a data structure.

1           103.    The method of claim 102, wherein  
2           said data structure is a permission list.

1           104.    The method of claim 102, wherein  
2           said data structure is a permission list entry.

1           105.    The method of claim 102, wherein  
2           said data structure is a pointer to a permission list.

1           106.    The method of claim 105, wherein said data structure further comprises:  
2           another pointer to another permission list.

1       107.   The method of claim 102, further comprising:  
2       employing permission list chaining in said data structure.

1       108.   The method of claim 102, further comprising:  
2       selecting a selected permissions matrix entry of said permissions matrix entries,  
3                wherein said selecting comprises  
4                identifying a row of said permissions matrix using a source user group  
5                identifier,  
6                identifying a column of said permissions matrix using a destination user  
7                group identifier, and  
8                identifying a permissions matrix entry of said permissions matrix entries in  
9                said row and said column as said selected permissions matrix entry.

1       109.   The method of claim 108, further comprising:  
2       selecting a permission list from a plurality of permission lists using said selected  
3       permissions matrix entry.

1       110.   The method of claim 108, further comprising:  
2       selecting a permission list entry from a permission list using said selected  
3       permissions matrix entry.

1       111.   A network comprising:  
2       a first network device, wherein  
3                said first network device is configured to generate a packet, and  
4                said packet comprises a source user group identifier.

1       112.   The network of claim 111, wherein  
2       said source user group identifier identifies a user group of said first network  
3       device.

1        113.    The network of claim 111, further comprising:  
 2        a second network device, wherein  
 3                said second network device is coupled to receive said packet,  
 4                said second network device comprises an access control list,  
 5                said access control list comprises an access control list entry, and  
 6                said access control list entry comprises a user group field.

1        114.    The network of claim 113, wherein  
 2        said second network device is configured to compare said source user group  
 3                identifier with a destination user group of a destination of said packet  
 4        said destination user group is identified by a destination user group identifier, and  
 5        said destination user group identifier is stored in said user group field.

1        115.    The network of claim 114, wherein said access control list entry further  
 2 comprises:  
 3        a plurality of user group fields, wherein  
 4                said user group fields further comprise  
 5                        a source user group field, and  
 6                        a destination user group field, and  
 7        said user group field is said destination user group field.

1        116.    The network of claim 113, further comprising:  
 2        a third network device, wherein  
 3                said third network device is coupled between said first and said second  
 4                network devices,  
 5                said third network device comprises a forwarding table,  
 6                said forwarding table comprises a plurality of forwarding table entries, and  
 7                at least one forwarding table entry of said forwarding table entries  
 8                comprises a user group field.

1           117. The network device of claim 116, wherein said at least one forwarding  
2 table entry further comprises:  
3           a port identifier field, wherein  
4                 a port identifier stored in said port identifier field identifies a port,  
5                 said packet is received on said port, and  
6                 a user group, identified by a user group identifier stored in said user group  
7                 field, is associated with said port.